

# TIBERIUS

## Rules of Behavior, March 2024

**Before you are granted access to the Centers for Disease Control and Prevention's Tiberius Platform (hereafter referred to as the "system"), you are required to read and acknowledge the following rules of behavior (RoB).**

**I will:**

Take all necessary precautions to protect system information and IT assets from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse.

Notify the helpdesk (tiberius-help@cdc.gov) if I believe I am being granted access to information or system functions to which I should not have access.

Notify the helpdesk if my position or role changes or I leave my organization/company so that my system access can be re-evaluated based on these changes.

Report all suspected or identified security incidents and privacy breaches to CDC's Security Incident Response Team (CSIRT) at [csirt@cdc.gov](mailto:csirt@cdc.gov) or 866-655-2245 as soon as possible, without unreasonable delay and no later than within one (1) hour of occurrence/discovery.

Log out of the system, lock my workstation and/or close my web browser when I am finished with my work.

Comply with applicable HHS/CDC policies, standards, guidelines; and with applicable executive orders, regulations, and laws.

Limit my usage of artificial intelligence (AI) to only the data, workflows, and use cases for which I have been approved.

Review AI-derived results, answers, responses etc. for accuracy and validity and make corrections as needed; especially if used in crucial and high-risk decision-making.

Clearly disclose any uses of generative AI, including model type and version, in presentations, publications, etc.

Provide feedback when prompted by the system. Feedback will help refine and improve the system and notify administrators when there are potential problems.

Review and follow the CDC's Generative AI Guidance (applicable to CDC staff only).

Take an AI course before accessing AI tools on Tiberius.

**NOT** make system interconnections to the system without an approved API Access Request or System Interconnection/Data Use Agreement.

**NOT** enter, upload, or otherwise cause Personally Identifiable Information (PII), beyond business contact information, to be added to this system. This prohibition includes personal contact information, such as personal mailing or home address, personal email address, and personal phone number as well as sensitive PII content such as protected health information (PHI).

**NOT** exceed authorized access to the system by any means including circumventing or bypassing security safeguards, policies, system configurations, or access control measures.

**I am aware that:**

Information in this system, including information I upload or enter, may be subject to the Freedom of Information Act (FOIA) and may become a permanent federal government record.

Information in this system may not be shared with the public without approval from the data owner(s).

System information may be shared within my organization (state, federal agency, public health department, etc.) for internal use only.

I am responsible for misuse or improper disclosure of any data I share.

Classified information may not be stored, processed, or transmitted via this system.

I have no expectation of privacy and I will be held accountable for my actions while using this system.

AI has limitations which include inheritance of biases from the model and training data, decision-making processes that may not be evident in the results, limited understanding of context, and models that are general and not often specific to the relevant knowledge domains.

AI can provide fake, false, or misleading information (sometimes referred to as "hallucinations").

**I have read the Tiberius RoB. I understand and agree to comply with the provisions stated herein. I understand that violations of these RoB may result in disciplinary action and that these actions may include termination of employment; removal or debarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment.**